SECURE AND PERSONALIZED BROADCASTING OF AUDIOVISUAL STREAMS BY A HYBRID UNICAST/MULTICAST SYSTEM

[0001] The present invention relates to the area of the broadcasting of digital audiovisual sequences.

[0002] The present invention proposes supplying a process and a system that permit the visual and/or auditory protecting of an audiovisual sequence stemming from a digital standard, a digital norm or a proprietary standard, its distribution in a secure manner in multicasting mode via a telecommunication network, and the reconstituting of its original content on a recomposition module of the addressed equipment from a protected digital audiovisual stream.

[0003] The present invention relates more particularly to a device capable of transmitting a set of high-quality audiovisual streams in a secure manner via a telecommunication network to a viewing screen and/or to an audio output belonging to a terminal or display device such as a television screen, a computer or a mobile terminal such as a telephone or PDA (Personal Digital Assistant), or the like while preserving the audiovisual quality but avoiding any fraudulent use such as the possibility of making pirated copies of the broadcast contents. The invention relates essentially to a process and a client-server system that protects the audiovisual contents by separating them into two parts, the second part of which is absolutely indispensable for the reconstitution of the original stream, which latter is restored as a function of the recombination of the first part with the second part.

[0004] The process used for the description of a preferred exemplary embodiment of the present invention separates the audiovisual stream into two parts in such a manner that the first part, called "modified main stream", contains the quasi totality of the initial information, for example, more than 99%, and a second part, called "complementary information", containing targeted ele-

ments of the initial information and which is of a very small size compared to the first part. The complementary information contains data extracted from the original stream, which extracted data is replaced by "decoys" in the modified main stream in such a manner as to cause a severe audiovisual degradation while keeping this main stream protected in conformity with the norm or standard of the original stream.

[0005] It is currently possible to transmit audiovisual programs in digital form via broadcasting networks of the microwave [herzian], cable, satellite type, etc. or via telecommunication networks of the DSL type (Digital Subscriber Line) or BLA type of (Local Radio Loop) or via DAB networks (Digital Audio Broadcasting) as well as via any wireless telecommunication network of the GSM (Global System for Mobile), GPRS (General Packet Radio Service), UMTS (Universal Mobile Telecommunication System), Bluetooth, WiFi types, etc. Moreover, in order to avoid the pirating of works broadcast in this manner these works are frequently encrypted or scrambled by various means well known from the prior art.

[0006] The prior art contains the document US 6,295,361 presenting a method and a device that permit a key management node to decide the process for changing the group key of certain nodes in a multicasting group with the aid of an indicator inserted into a multicast packet. The management node decides how to insert the indicator and which nodes are concerned. The new key is then sent and when all the nodes of the group have received their key, the management node sends an indicator or also a date from which all the members of the group are authorized to use the new keys. This prior art represents a method for managing the multicast session with the aid of dynamic changing of the group keys. The same key is attributed to all the members of the same group with the aid of which the data is decrypted. However, the protection used is the encryption and all the data initially present in the audiovisual stream remain in the protected

stream. Consequently, this prior art does not resolve the problem of high security and personalization, the subject matter of the present invention.

[0007] The prior art also makes reference to the document WO 02/11356 A2, that presents a method for the managing of keys between the client and the server in a multicast environment. The method is based on the establishing of a secure channel between the server and the client using an SSL protocol (Secure Socket Layer) or TLS (Transport Layer Security) with certain modifications of the order of the exchanging of messages in order to be able to generate a management key and to send this key to the client via the secure channel, from which key the client generates the future key for the session with the server. The clients of one and the same multicasting group use the same management key for generating a session key during the communication session. This prior art does not correspond to the criteria for the secure transport of audiovisual data, subject matter of the present invention, and the data, even the encrypted data, is integrally present in the protected data stream.

[0008] In distinction to the state of the prior art the present invention proposes a system characterized by the multicast broadcasting of the complementary information and in that a processing is carried out in real time on segments representing entities that are independent as regards the processing, which segments comprise data for the reconstruction of complete audiovisual information and are secured and personalized for each user and are sent to the equipment of the addressees in real time via a low-bandwidth network from a central server functioning as access controller for the viewing of the contents.

[0009] In the present invention the term "multicast" denotes a manner of transmitting from a sender to all the receivers belonging to the same group of subscribers in contrast to the term "unicast", that represents a manner of transmitting from a sender to a single receiver.

[0010] The protection applied to contents distributed by the secure multicasting system, subject matter of the present invention, is based on the principle of deleting and replacing certain information present in the original encoded audiovisual signal by any method, e.g., substitution, modification, permutation or shifting of the information. The solution consists in extracting and permanently preserving in a secure server this complementary information containing a part of the original audiovisual stream, which part is indispensable for reconstituting this audiovisual program but has a very small volume relative to the total volume of the audiovisual program recorded at the user's or received in real time by this user. This complementary information is transmitted in multicasting mode via the secure transmitting network at the moment of viewing and/or hearing of this audiovisual program.

[0011] The fact of having removed and substituted by decoys a part of the original data of the initial audiovisual stream during the generation of the modified main stream does not permit the restitution of the original stream from this modified main stream, that is entirely compatible with the format of the original stream and can therefore be copied and read by a classic reader. This modified main stream is, however, completely incoherent from the viewpoint of human auto visual perception.

[0012] As the original digital stream is separated into two parts, the largest part of the audiovisual stream, said modified main stream, will therefore be transmitted via a classic broadcasting network whereas the lacking part, said complementary information, will be sent on demand via a narrow-band telecommunication network or via a physical support such as a memory card, disk, etc. However, the two networks can be combined while keeping the two transmission paths separate. For the reconstitution of the original stream the complementary information is sent piece by piece during the viewing and/or hearing of the audiovisual stream.

[0013] The subject matter of the present invention is the secure and personalized transmission, after authentication of the user, of the complementary information in multicasting mode in such a manner as to avoid it from being able to be copied or fall entirely into the possession of the user or of any ill-disposed person.

[0014] Multicast distribution is used in the instances in which a large number of users wish to access the same content at the same time, which is, e.g., the case for direct broadcasting by satellite or cable or via any other network that allows several subscribers to be accessed at the same time. The content stream is transmitted from a server to the clients via a multicasting channel. The complementary information designated and personalized for each active client (member of the multicasting group) is broadcast by a separate path from a secure server also in multicasting. The user who is interested in a content joins the multicasting group, receives the complementary information as a function of his rights, which thus allows the reconstitution of the original stream and therefore the viewing simultaneously with the reception of this complementary information.

[0015] On the one hand, the benefit of the distributing in multicasting mode of the complementary information is that a central server can model its distribution to a very large number of consumers. On the other hand, the disadvantage of distributing in multicasting is that the same complementary information is transmitted to all the users in the group and as a consequence it is more difficult to individually control the different consumers.

[0016] From the standpoint of security and content protection, multitasking has the disadvantages of the models "one-to-many" or "a single sender, several receivers" from the English expression "one-to-many" that designates a communication operation from a single sender and

directed to multiple receivers. This creates the necessity for working out a protection system for reliable multicasting distribution based on the following characteristics:

- The solution of the present invention is complementary to the multicasting distribution protocol "join/leave the group" that is well-known to an expert in the art.

- The making of the decision to join/leave the group is performed at the level of the access elements of the network for access control from a previously established list where the client receives the permission to join this group but does not have the right at this stage to view the stream broadcast for this group, which access elements are called switches.

- The users for which a switch refused authorization cannot join the group.

- The central server is responsible for updating the client list and for making the decision to include new identities in the list of encryption keys for the session after a first stage of authentication with the client desiring to join the group.

- Each session key is individual for each client and has its own lifetime, after which it is considered as a non-valid key and is then destroyed by the server.

- The scale of a multicasting group is on the order of several thousand users per group.

- The relation is of the one-to-all type in a single direction. Consequently, the server is always the emission source and the clients are always the receivers with the exception of requests emitted from the receivers to the server via a unicasting return link or, e.g., during the authentication stage.

[0017] The particularity of the present invention is that the server broadcasts in multicasting to a large number of users that can join and leave the group in a dynamic manner. Furthermore, in the present invention the functionality of the selective relation ("push relation" in English) is

eliminated, that is, the clients of one and the same group can not communicate with each other and as a consequence the model of the multicasting connection is simplified, as well as the protocol for the management and distribution of keys for the members of the group.

[0018] The subject matter of the present invention is a simplified protocol for the secure broadcasting of the complementary information in multicasting, thus completing the existing multicasting broadcasts protocols with a secure broadcasting protocol of said complementary information.

[0019] To this end the invention relates according to its most general meaning to a process for the secure distribution of digital audiovisual streams according to a standard, normalized or proprietary format, in which streams a separation of the stream into two parts is made prior to the transmission to the addressee's equipment in order to generate a modified main stream with the format of the original stream and to generate complementary information with any format comprising the digital information suitable for permitting the reconstruction of the original stream, characterized in that this modified main stream is transmitted from a distribution server via separate paths during the distribution phase and that this complementary information is transmitted in multicasting mode to this addressee's equipment from a secure central server passing via at least one router and at least one switch connecting this addressee's equipment to this central server via at least one access point.

[0020] The authentication between the client and the server is preferably performed in unicast mode.

[0021] According to a particular embodiment a session key that is unique by content and by client is generated by the central server following this authentication.

[0022] The complementary information is advantageously compressed and encrypted prior to being sent to the client.

[0023] According to a variant the management of a multicasting group is performed in the connection layer controlling the distribution of data in multicasting solely for the access point concerned.

[0024] The managing and the securing of the complementary information is preferably performed following a multi-reception of the requests for authentication by a central server and comprises a compression stage, and encryption stage and a management stage of said session keys.

[0025] According to a preferred embodiment the regeneration of a new session key for the client is performed as a function of the decision of the client to prolong the connection, is based on the lifetime of the preceding session key and is individual for each member of the multicasting group.

[0026] According to another embodiment the complementary information is secured and personalized for each client and for each multicasting session with the aid of methods of hybrid or symmetric or asymmetric encryption.

[0027] The invention also relates to a system for the secure distribution of audiovisual streams, characterized in that the control of the throughput in the multicasting group is performed as a consequence of the managing and personalizing of the securing of the complementary information.

[0028] The system of the invention preferably comprises a device for separating the original video stream into a modified main stream and into complementary information, at least one multimedia server containing the protected audiovisual streams, at least one secure central server

comprising a device for securing and personalizing this complementary information from which the complementary information is distributed, at least one telecommunication network, at least one router, at least one switch functioning as access point for the connection to the addressee's equipment and a device in the addressee's equipment for the reconstruction of the original audio-visual stream as a function of said modified main stream and of said complementary information.

[0029] The present invention will be better understood with the aid of the exemplary embodiments and of the following detailed stages.

[0030] A preferred but non-limiting exemplary embodiment of the process that responds to the criteria of security and reliability is illustrated by the client-server system presented in the figure.

[0031] The auto visual stream in digital form 1 transmitted via link 6 to analysis and scrambling module 2 is separated into two parts by this module 2. Modified main stream 17 is stored in multimedia server 16 and is sent in real time to the client during viewing via a broadband network or is stored in advance on the backup device of terminal 14 of the user. Complementary information 3 is sent to storage and segmentation module 41 of secure central server 4.

[0032] Since the complementary information is sent solely on demand, its distribution in real time, its securing and its personalizing for each user is realized by virtue of the property of "scalability in throughput" on the transport networks. The notion of "scalability in throughput" is defined as the capacity of a network to manage, modify, allocate and adapt the throughput of the transiting streams as a function of the bandwidth that is available or negotiated and as a function of the network congestions. As a result of the low throughput of the complementary information transmitted in real time, the process of the present invention contains a segmentation stage of the complementary information in module 41, which generates data segments of variable

size with each segment corresponding to an entire, subjectively coherent audiovisual element such as an image or a frame, a group of images or GOP ("Group Of Pictures" in English) in an MPEG-2 stream for example. In a variant the segmentation is performed in a single stage after the generation of said complementary information 3 and produces a series of segments designated as "stream of complementary information" that remain stored in storage and segmentation module 41. In another variant the stream of complementary information is generated in real time.

[0033] The segmentation stage of the complementary information is followed by a stage of encapsulation en blocks of data and an encryption stage in module 42 preceded by a stage of compressing their size in which the blocks remain available on demand by the users. The stream of complementary information is continuously sent to terminal 14 of the user in the form of blocks with a block containing a segment to which access information or "header" was added comprising data relative to the identity of the user in the case of a classic centralized network. The header preferably comprises data relative to the mobility of the user (position, rights, network access points, for example) in the case of a distributed network. The header advantageously comprises data relative to the encryption keys of the stream of complementary information. A block is the fundamental unit of communication and is also called UFIC (French "Unite de Flux d'Information Complementaire" = English "Unit of Stream of Complementary Information").

[0034] When the user "i" wishes to view a sequence he connects via his equipment 14i and link 13i to his closest access point, switch 12a, that previously gave him the authorization to join the multicasting group. Switch 12a redirects the request via a link 11 to local router 10a, which latter for its part directs the request via link 9a to central router 8, which central router 8

addresses central server 4 via link 7. When server 4 thus receives the request of client 14i, central server 4 requires an authentication from this client 14i in order to make a decision about sending the UFIC's requested, that are unique as an audiovisual sequence. After the authentication dialog, the identification of the client 14i by central server 4 that he is in its database 5, and the generation of a unique session key, the stream segmented in module 41 is sent via link 43 to module 42, compressed and encrypted in this module 42 by said unique session key by heading and by client. The UFIC's are then transported via link 7, central router 8, link 9a, local router 10a, link 11a, switch 12a and link 13i to terminal 14i of the user i. Terminal 14i of the user is advantageously equipped with a smart card 15i on which the description of the units of the stream of complementary information is performed.

[0035] Switch 12a is responsible for the security and controls the addresses of the clients in the access list composed of information relative to the previous sessions with the client (e.g., time and duration of connection, anticipated or delayed payment, type of contents viewed), which assures the personalizing of each client session and therefore of the complementary information by forming UFIC units. One embodiment is the use of a hybrid method such as, e.g., using unicasting for authentication with the aid of secure keys and multicasting for the broadcasting of the complementary information.

[0036] In the first place, if the client 14i succeeds in joining the multicasting group desired via switch 12a, it is because he has a recognized identity and an authorization from the network to receive these packets of complementary information after the authentication stage; however, if no valid session key was generated by the central server, the client can not use the UFIC's, which UFIC's are broadcast and encrypted solely with the keys of the other users 14j, 14k, etc.

[0037] In the second place, the client communicates with the server of complementary information 4 in a point-to-point link in unicasting and the authentication phase is thus performed in order to assure that the client has sufficient rights for receiving the UFIC's and for generating the session key (via a secure method of exchange of information) and the viewing rights are backed up in a database for managing rights 5.

[0038] At the end of this stage server 4 automatically adds the new key of client 14i into the list of session keys corresponding to the multicasting group requested.

[0039] Server 4 begins to encrypt the current UFIC with the session key and sends the UFIC with what is called a label that is delivered to the client during the authentication stage. This label contains the information about a unique association between the encrypted UFIC and each client. Client 14i receives groups of packets and retains said valid label and decrypts the data portions with said session key until the lifetime of this session key expires.

[0040] After a period that is sufficiently long to have the right to request a new key and in the instance in which the client desires to continue receiving the complementary information of the same multicasting group, a new authentication stage recommences.

[0041] Server 4 advantageously encrypts the UFIC's corresponding to a simultaneous broadcasting of the same content with the session keys of all authorized clients 14i, 14j, 14k, ..., 14q and sends the same encrypted UFIC a certain number of times with each key different, corresponding to the numbers of clients connected.

[0042] A compression of the units of streams of complementary information is preferably applied prior to the encryption with all the session keys, which reduces the volume of information to be transported and also increases the security of the encrypted UFIC's as a consequence by reducing the redundancy because many cryptographic analyses exploit the redundancy in

order to break the protection. The efficacy of the compression algorithm is also one of the factors that manages the throughput scalability of the multicasting group as a function of the number of members per group.

[0043] Each user decrypts the UFIC's received with the aide of his own session key.

[0044] The term "transmission cycle of the server" denotes the stage of sending a UFIC in compressed form, encrypted with all the keys of the members of the group to the address and the port number of the multicasting group.

[0045] An advantage of this technique is that it assures a resistance to pirating due to the fact that a multiple encryption of the same content is applied with different keys for the different addressed equipments. The compression mechanism is applied for the transmission cycle of the server in order to avoid a traffic that is too high for the groups with a large number of members (several thousand users). This model is suitable for being used for any lossless compression algorithm of the LZ (Lempel-Ziv) type, e.g., LZW (a variant of LZ by Terry Welsch), LZJH (Lempel-Ziv-Jeff-Heath or v.44 by ITU-T).

[0046] Periodic renewals of the session keys are made in order to assure their cryptographic security. For example, a session key can be valid for a period of two hours, during which the key deciphers a quantity of UFIC's with a throughput of a dozen of kbits/s equal, e.g., to 2^{20} data blocks, each with a length of 64 bits.

[0047] An extension of the function of observing messages of the multicasting group ("snooping" in English) with the IGMP (Internet Group Management Protocol) protocol at the last distribution point 12 is used in the connection layer for access management (authorize or prohibit) for each client on the streams for which this client has or does not have rights, and as a consequence optimizes the bandwidth for each client at his access point such as, e.g., a DSLAM

(Digital Subscriber Line Access Multiplexer) of a DSL (Digital Subscriber Line) network. This extension of the observation function thus adds an extended and secure mode of multitasking transmission. This complementary information is thus transmitted during the distribution phase in an extended and secure mode of multitasking transmission to said addressee's equipment from a secure central server passing through at least one router and at least one switch connecting this addressee's equipment to this central server via at least one access point. The system keeps the personalization of the UFIC's for each client while reducing the number of unicasting connections per server with the exception of moments of authentication. The system also optimizes the throughput, therefore, the quantity of data to be transmitted as a function of the variation of the number of clients per group. Thus, the access management and the personalization of the complementary information "UFIC" control the throughput in the multicasting group. The current version of the IGMP protocol allows switches 12 to detect the IGMP messages of the member clients, to send the respective response and to control the distribution of packets in multitasking up to the port of the client. In the present invention this function is completed by a filtering relative to the first control level with a list of addresses of the MAC (Medium Access Control) connecting layer, which addresses represent the clients authorized to connect to the multicasting group.

[0048] Furthermore, a marking with a label is added for each compressed and encrypted data packet that represents the identity of the client and also a second level of control and of personalization.

[0049] This identity is used by switch 12 to determine the physical port to which the packets are distributed by sending the client in question only the packets marked with his own label.

[0050] According to a variant the UFIC's are encrypted with the aid of symmetric encryption algorithms and the encryption key is then encrypted with a public key of the addressee. This is a hybrid authentication mode.

[0051] According to another variant the UFIC's are encrypted with the aid of asymmetric encryption algorithms and this is a PKI ("Public Key Infrastructure" in English) authentication mode.

[0052] The present invention will be illustrated with the aide of a preferred second exemplary embodiment that includes a multicasting protocol, a mutual authentication method and a compression method for the server comprising multicasting protocols used and their extension for the distribution of the complementary information, subject matter of the present invention.

[0053] The multicasting transmission system is based on a group management protocol (IGMP) that is responsible for the control for joining/leaving the multicasting group. This protocol is executed between the client 14i, 14j, 14k and his closest network access point, switch 12a. A multi-casting routing protocol controls the routing of the multicasting traffic from switches 12 to all routers 10 of the distribution network.

[0054] A control processor located in switch 12 observes the IGMP messages sent by clients 14. The switches capable of managing and emulating IGMP messages also use this information for dynamically configuring their own observation filters.

[0055] This solution optimizes the managing of the bandwidth at the level of the switches, avoiding an overloading of the LAN's ("Local Area Network"in English), in particular in the instances in which the final user switches frequently from one multicasting group to another one, e.g., when changing a television channel.

[0056] Routers 10 supporting multicasting routing, and switches 12 for which layer 3 of the OSI model is capable of managing the data used for this example, contain a bandwidth control with a functionality of limiting throughput in IP multicasting that allows an upper limit to be imposed for the traffic carried out from the server to the multicasting groups. The mechanism for defining the limits includes the definition of a multicasting source filter and a multicasting group receiving filter per reception port. This control filter is based on the IP address or also on the Mac address (address of the network card "Medium Access Control") using, e.g., the MVR (Multicast VLAN Registration) mechanism, and as a consequence in order to avoid a fraudulent attribution ("spoofing" in English) of the IP network address of the client a complementary protocol is applied in unicast "Unicast Reverse Path Forwarding" (URPF) between client 14 and switch 12.